Davis Wright Tremaine LLP

1919 Pennsylvania Avenue N.W.
Suite 800
Washington, D.C. 20006-3401

Helen Foster
(202) 973-4223 tel
helenfoster@dwt.com

October 11, 2019

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Re: Security Breach Notification

Dear Office of the Attorney General:

I am writing you on behalf of Davis Wright Tremaine, LLP (DWT), located at 920 Fifth Avenue, Seattle WA 98104, pursuant to Md. Code Ann. Comm. Law 14-3504.

On August 27, 2019, Matrix Trust Company (Matrix), a vendor that serves as the trustee and custodian for some DWT benefits programs, uploaded a file to its secure web portal with information related to check distributions. On August 28, 2019, this information was inadvertently made accessible to and viewed briefly by a single employee of a company that also uses Matrix's services. That employee downloaded the file and shared it with a second employee, believing it to be a file intended for his company. Once the employees identified that the information was provided to them in error, they contacted Matrix. Matrix has since secured written confirmation that the file was permanently deleted and is not retained in any form.

On September 12, 2019, Matrix Trust Company contacted DWT by letter to inform DWT of the incident. The initial communication stated that "in some instances" Social Security numbers were included in the file. On Thursday, September 19, 2019, DWT confirmed that the file contained Social Security numbers for all listed individuals, in addition to payment dates, payments amounts, payee names, and payee addresses. Matrix Trust Company investigated the incident and determined it was the result of one of its employees failing to follow its established procedures for secondary review prior to transmission of sensitive information.

* * *

Davis Wright Tremaine LLP

1919 Pennsylvania Avenue N.W.
Suite 800
Washington, D.C. 20006-3401

Helen Foster
(202) 973-4223 tel
helenfoster@dwt.com

Based on the investigation to date, DWT has confirmed that the personal information of nine (9) Maryland residents may have been impacted by the incident. DWT has found no evidence that the personal information was misused. DWT will send written notice by U.S. mail to impacted individuals on October 14, 2019. A copy of this notice is enclosed. As referenced in the letter, consumers will be provided with **12 months** of credit monitoring to affected consumers through **Kroll**.

Sincerely,

Helen Foster
Chief Privacy Officer

Davis Wright Tremaine LLP

Suite 800
1919 Pennsylvania Avenue N.W.
Washington, D.C. 20006-3401
Helen Foster
(202) 973-4223 tel
helenfoster@dwt.com

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to tell you about a data security incident that occurred with one of our vendors and that resulted in the unauthorized access to and/or acquisition of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident. We believe there is little risk that your information will be misused as a result of this incident. In an abundance of caution, however, we are providing you with identity protection services, as described below.

WHAT HAPPENED?

On August 27, 2019, Matrix Trust Company, a vendor that serves as the trustee and custodian for some of our benefits programs, uploaded a file to its secure web portal with information related to check distributions. On August 28, 2019, this information was inadvertently made accessible to and viewed briefly by a single employee of a company which also uses Matrix's services. That employee downloaded the file and shared it with a second employee, believing it to be a file intended for his company. Once the employees identified that the information was provided to them in error, they contacted Matrix Trust Company. Matrix Trust Company has since secured written confirmation that the file was permanently deleted and is not retained in any form. Matrix Trust Company believes that there is little to no risk to you from this incident.

On September 12, 2019, Matrix Trust Company contacted DWT by letter to inform us of the incident. DWT confirmed that the file contained Social Security numbers for all listed individuals.

WHAT INFORMATION WAS INVOLVED?

Information in the accessed file included payment dates, payment amounts, payee names, payee addresses, and participant Social Security numbers.

WHAT WE ARE DOING?

Matrix Trust Company investigated the incident and determined it was the result of one of its employees failing to follow its established procedures for secondary review prior to transmission of sensitive information.

We have also secured the services of Kroll to provide identity monitoring at no cost to you. The following identity monitoring services are available and you can activate at any time during the activation period.

Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.
*You have until **January 9, 2020** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

WHAT YOU CAN DO:

Although our investigation has not found that your information has been misused, we treat this matter with the utmost seriousness and want to ensure that you have the necessary information to take preventive steps to help protect yourself from identity theft.

Please note: Following activation, additional steps are required by you in order to activate your fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Please review the enclosed "Steps You Can Take to Further Protect Your Information" section included with this letter. This section describes additional steps you can take to protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

As always, we encourage you to regularly review and monitor your financial statements and credit reports, and report any suspicious or unrecognized activity immediately. You should be vigilant for incidents of fraud and identity theft and report any suspected incidents of fraud to the relevant financial institution, local law enforcement, your state Attorney General, or the Federal Trade Commission.

FOR MORE INFORMATION:

Further information about how to guard against identity theft appears on the next page. Should you have any questions, please contact 1-866-775-4209, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. national holidays).

We deeply regret any inconvenience this may cause you.

Sincerely,

Helen Foster
Chief Privacy Officer

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Obtain a Copy of Your Credit Report. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 10528
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Place a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for up to a year. Identity theft victims can also get an extended fraud alert for up to seven years. Military members have additional benefits and should contact the credit reporting agencies for further questions. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Place a Security Freeze on Your Credit File. As of September 21, 2018, a new federal law allows consumers to freeze and unfreeze their credit file free of charge at all three major credit bureaus. A freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each consumer reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorney General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Penn. Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.